WHAT IS CLAIMED IS:

1. A packet cryptographic processing proxy apparatus connected between the Internet and a terminal, comprising:

a cryptographic communication channel information storage part which stores cryptographic communication channel information used for establishing a cryptographic communication channel at least for packet communication on the Internet, in packet communication between a counterpart apparatus connected to the Internet and the terminal; and

cryptographic processing means for performing cryptographic processing for a received packet based on the cryptographic communication channel information stored in said cryptographic communication channel information storage part.

2. The packet cryptographic processing proxy apparatus according to Claim 1, further comprising:

a filter information storage part which stores sending source identification information, sending destination identification information, protocol information indicating a packet communication procedure and processing instruction information indicating whether or not to perform cryptographic processing, as filter information; and

cryptographic processing determination means for, by referring to said filter information storage part based on filter information in a packet received by the packet cryptographic processing apparatus, determining whether or not to perform cryptographic processing of the received packet by said cryptographic processing means based on the processing instruction information.

3. The packet cryptographic processing proxy apparatus according to Claim 1, further comprising a received packet determination part

which determines whether or not a packet received from the counterpart apparatus is valid.

4. The packet cryptographic processing proxy apparatus according to Claim 1, wherein said cryptographic communication channel information storage part includes a detachable, tamper-proof device in which at least part of the cryptographic communication channel information is stored.

5. The packet cryptographic processing proxy apparatus according to Claim 1, wherein said cryptographic communication channel information storage part includes a storage medium in which at least part of the cryptographic communication channel information is changeable.

6. The packet cryptographic processing proxy apparatus according to any of Claims 1 to 5, being logically directly connected to a network interface device of the terminal.

7. The packet cryptographic processing proxy apparatus according to any of Claims 1 to 5, being implemented on a device which is connected between the Internet and the terminal and which does not have an IP address.

8. The packet cryptographic processing proxy apparatus according to any of Claims 2 to 5, further comprising a terminal information collection part which collects a part of at least one of the cryptographic communication channel information and the filter information and stores the information in said filter information storage part.

9. The packet cryptographic processing proxy apparatus according to Claim 1, further comprising:

a packet determination part which determines from a received packet whether or not to agree with the counterpart apparatus on

cryptographic communication channel information for establishing a packet communication channel between the counterpart apparatus and the terminal;

a cryptographic communication channel information agreement part which, if the packet determination determines necessity of agreement, makes the agreement and stores the agreed cryptographic communication channel information in said cryptographic communication channel information storage part; and

a key information setting part which sets key information for performing cryptographic processing of a packet, in the cryptographic communication channel information agreed by said cryptographic communication channel information agreement part, for the terminal.

10. The packet cryptographic processing proxy apparatus according to Claim 9, wherein, if determining necessity of agreement on cryptographic communication channel information, said packet determination part determines whether valid cryptographic communication channel information corresponding to the received packet is stored in said cryptographic communication channel information storage part, causes said key information setting part to set key information in the cryptographic communication channel information for the terminal if the valid cryptographic communication channel information is stored, and causes said cryptographic communication channel information agreement part to make agreement on cryptographic communication channel information if the valid cryptographic communication channel is not stored.

11. The packet cryptographic processing proxy apparatus according to Claim 10, wherein, if said packet determination part determines necessity of agreement on the cryptographic communication channel information, and address information in the received packet is stored in said

filter information storage part, said packet determination part causes agreement on the key information to be made.

12. The packet cryptographic processing proxy apparatus according to Claim 11, further comprising a terminal information acquisition part which detects the terminal, acquires address information from the terminal and stores the acquired address information in said filter information storage part.

13. A packet cryptographic processing method comprising the steps of:

(a) storing cryptographic communication channel information used for establishing a cryptographic communication channel at least for packet communication on the Internet, in packet communication between a counterpart apparatus connected to the Internet and a terminal, in a cryptographic communication channel information storage part under agreement with the counterpart apparatus; and

(b) performing cryptographic processing for a received packet based on the cryptographic communication channel information.

14. The packet cryptographic processing method according to Claim 13, wherein the step (b) comprises the steps of:

(b-1) by referring to a filter information storage part based on filter information in the received packet, determining whether or not to perform cryptographic processing for the received packet; and

(b-2) causing the cryptographic processing to be performed if it is determined by the determination that cryptographic processing is to be performed, and causing the received packet to immediately pass or to be discarded if it is determined by the determination that cryptographic processing is not to be performed.

15. The packet cryptographic processing method according to Claim 13, wherein the step (a) comprises the steps of:

(a-1) determining whether or not a received packet requires agreement on cryptographic communication channel information and, if agreement is required, making agreement, for packet communication between a counterpart apparatus connected to the Internet and a terminal, with the counterpart apparatus on cryptographic communication channel information for performing cryptographic processing of a packet transmitted with the counterpart apparatus;

(a-2) setting the agreed cryptographic communication channel information for the terminal; and

(a-3) if agreement is not required, bypassing or discarding the received packet.

16. The packet cryptographic processing method according to Claim 15, wherein the step (a-1) comprises the steps of:

(a-1-1) determining whether valid cryptographic communication channel information corresponding to the received packet is stored in the cryptographic communication channel information storage means; and

(a-1-2) if the cryptographic communication channel information is stored, setting key information in the cryptographic communication channel information for the terminal; and, if the cryptographic communication channel information is not stored, making agreement on the cryptographic communication channel information, storing the agreed cryptographic communication channel information in the cryptographic communication channel information storage part as well as setting the agreed cryptographic communication channel information for the terminal.

17. The packet cryptographic processing method according to

Claim 16, wherein the step (a-1-1) comprises a step of, if agreement on cryptographic communication channel information for the packet is required, determining first whether address information in the received packet is stored in a filter information storage part; and, if the address information is stored, performing the determination about whether valid cryptographic communication channel information is stored in the cryptographic communication channel information storage part.

18. A readable recording medium on which a program for causing a computer to perform the packet cryptographic processing method according to any of Claims 13 to 17 is recorded.